Smart Grid, Security and EDA

Ingrid Verbauwhede, Patrick Schaumont
KULeuven – COSIC, Virginia Tech – SES

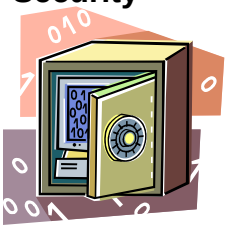
E-mail: ingrid.verbauwhede@esat.kuleuven.be
schaum@vt.edu

Acknowledgements:
current and former Ph.D. students at K.U.Leuven and UCLA

Energy, security and EDA

Energy

Security



EDA

Overview

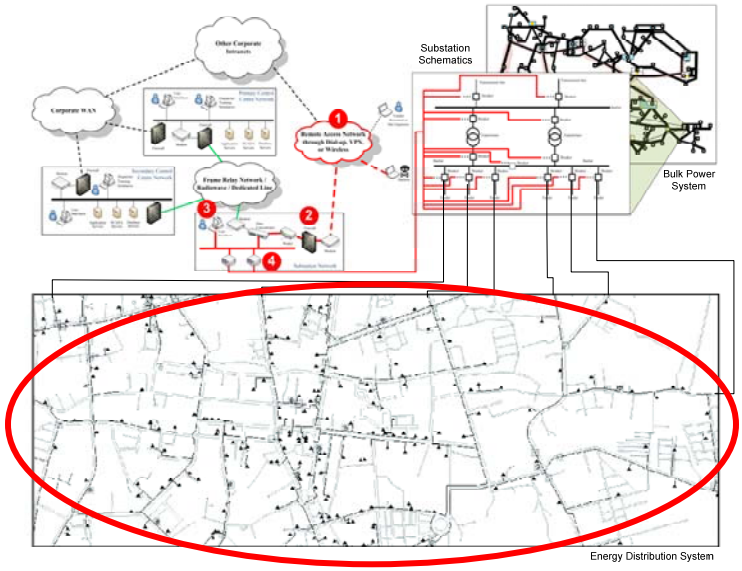
- Part I: Energy life-cycle
  - Focus on distribution
  - Smart meters & ICT infrastructure
- Part II: Security architecture
  - Risks
  - Security solutions: An example from road toll charging
- Part III: Implementation issues
  - Computational security
  - Physical security
  - Messages for EDA

Part I: Lifecycle of 'energy'

- Generation: nuclear plants, solar stations, …
- Transmission:
  - from generation to distribution to the users
  - Few players: US has three main networks (East, West and Texas)
  - goal is to keep the network stable (no matter what). Security is related to protocols to share data in case of emergency.
- Distribution:
  - Electronics needed at end points = Focus

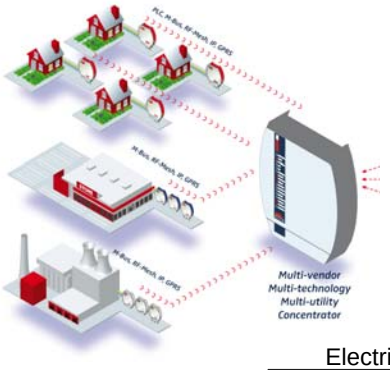
[source: C. Troncoso]

Our focus: distribution



Distribution: ICT system

Data generation



Data collection

Electricity usage →

← Billing rates

User can adapt consumption

Utility companies can adapt production (and billing rates)

Who wants Smart Meters? Stakeholders

- Government
  - Interest
    - Energy Problems: CO2 reduction
  - Role
    - Establishing policies, ensure reliable infrastructure
- Industry (chip manufacturers, GSM providers, energy distributors, Google's)
  - Interest
    - New business opportunities
  - Role
    - Provide infrastructure
- Users
  - Interest
    - Energy economics
  - Role
    - Using the system but…
    - privacy at risk

[adapted from: C. Troncoso]

Part II: Security and privacy

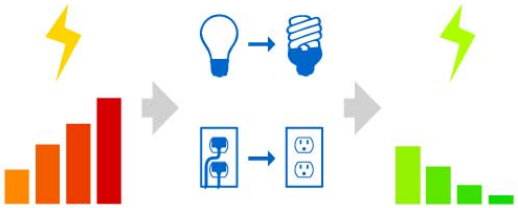
Dutch newspaper (NRC Handelsblad): "Smart energy meter will not be compulsory"

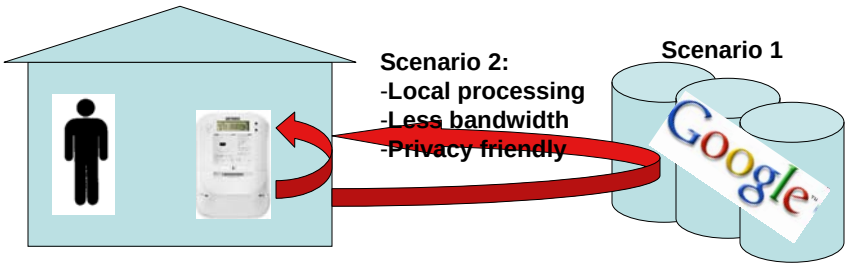
The 'smart energy meter' will not be compulsory in the Netherlands. Minister of economic affairs Maria van der Hoeven backed down after consumer groups raised privacy concerns.

[http://www.nrc.nl/international/article2207260.ece/Smart_energy_meter_will_not_be_compulsory]

Example: Google powermeter

"Save energy
- Save money
- Make a difference"





Smart Meter: Risks

- Example 1: "Your fridge consumes 4 times more electricity than average in your neighborhood, consider buying a new fridge."
  → can also be inferred locally.
- Example 2: "You arrive at home around 6pm, turn on the lights, start cooking (stove is on). Can someone call you about this new fridge (during dinner) ?"
  → useful information for phone marketing/sales.
  → also useful for burglars and hackers

Security Elements in a Smart Meter

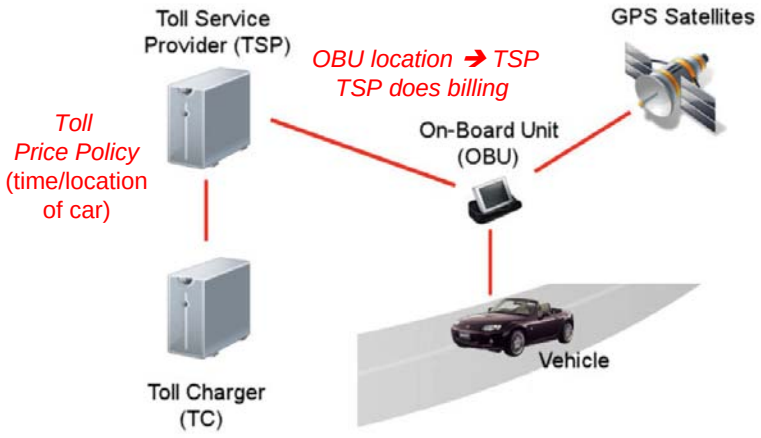
- Security ***protocols***
  - Confidentiality, authentication, integrity
  - Privacy
  - Key management
  - Secure updates of meters
  - …
- Secure ***implementations***
  - Efficient implementation of security protocols on embedded devices (smart meters)
  - Secure implementations, tamperproof, resistant to active and passive attacks

Similar use case: Road Charging

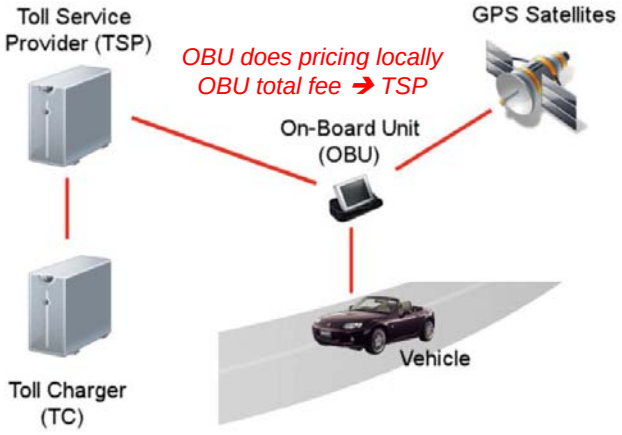
- Nowadays drivers pay flat fees for driving
- Satellite-based road charging
  - Drivers pay according to their road use
  - On-Board Unit (OBU) collects GPS location data
  - Typical policy: fee depends on road and time
- Main applications so far:
  - Pay-As-You-Drive (PAYD): insurance companies
  - Public Road Pricing: European Electronic Toll Service (EETS)
- Straightforward architecture
  - OBU sends location data to Service Provider
  - **Privacy** issues: fine-grained location data disclosed

[slides courtesy: Josep Balasch]

EETS straightforward implementation

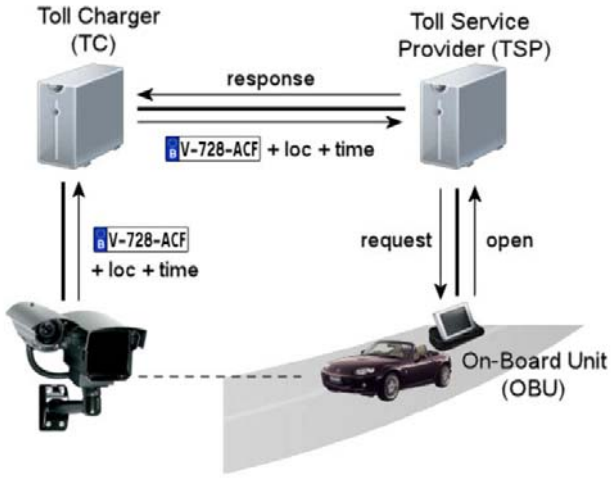


PrETP - Privacy Friendly Toll Pricing



PrETP – Verifying Security Concerns

- No personal data leaves the domain of the user!



Law enforcement

- Technical means do not suffice
  - OBU in hands of the user
- Instead technology can help:
  - Detect vehicles with inactive OBUs
  - Detect vehicles reporting false location data
  - Detect vehicles using incorrect road prices
  - Detect vehicles reporting false final fees
- Combination of law + technology

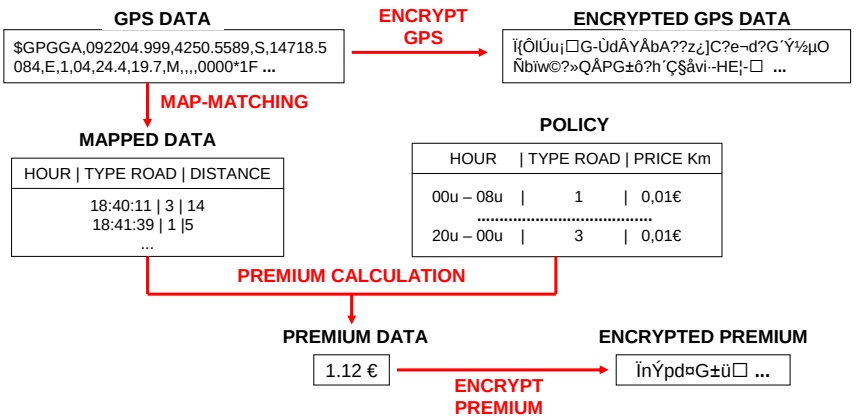
[slide courtesy: C. Troncoso]

Apply to smart meter

- Technical means do not suffice
  - ‘Smart meter’ in hands of the user
- Instead technology can help:
  - Detect homes with inactive smart meters
  - Detect smart meters reporting false energy data
  - Detect smart meters using incorrect energy rates
  - Detect smart meters reporting false final fees
  - . . .
- Combination of law + technology

Embedded Solution

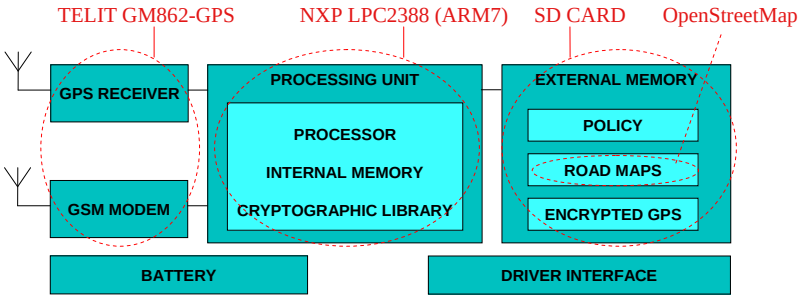
- Focus on normal mode of operation
- Focus on feasibility for embedded platform



[slides courtesy: Josep Balasch]

Embedded Solution

- OBU elements



- Minimize cost:
  - Off-the-shelf hardware components
  - Free licensed software tools

[slides courtesy: Josep Balasch]

Performance

- Test Scenario
  - Compressed road map of Belgium in SD Card
  - Cryptographic RSA keys 2048 bits
  - Constraint: process data upon GPS reception
- Timing results
  - One hour journey (one GPS string/sec)

	OPERATION	TIME @ 72 MHz
REAL-TIME	Map-Matching	0.328 seconds
OFF-LINE	Premium Calculation	0.096 seconds
	GPS Encryption	10.691 seconds
	Encrypt Premium	6.445 seconds

[slides courtesy: Josep Balasch]

Part III: Design methods to support trust in constrained devices

- Covered just one use case, i.e. privacy of the end-user

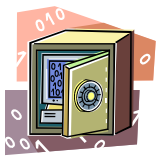
  There are many more security requirements: authentication, encryption, ..

- Demonstrated *feasibility* on an embedded processor
  In general: building security into ICT systems need:
  - building blocks for cryptography
  - building blocks for physical trust
  - Security protocols

Embedded Security

NEED BOTH

1 Efficient, lightweight implementations
- Within power, area, timing budgets
- Public key: 2048 bits RSA, 200 bit ECC on 8 bit μC and 100 μW
- Public key on a passive RFID tag

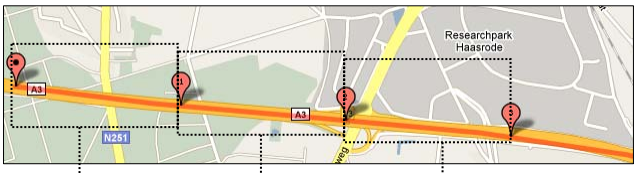


2 Trustworthy implementation
- Resistant to attacks
- Active attacks: probing, power glitches, JTAG scan chain
- Passive attacks: side channel attacks

1 Security vs. efficiency

- Computational security: number of bits
  - ECRYPT Yearly Report on Algorithms and Key Lengths (2010 version)
- Ex. Road tolling: cryptographic commitments
  - Each segment has assigned a price per Km p_i
  - This price is specified by the policy, assuming:

$$p_i = f\ (\ type\ road,\ time\ day\ )$$



Payment Tuple 1 | Payment Tuple 2 | Payment Tuple 3

 [slides courtesy: Josep Balasch]

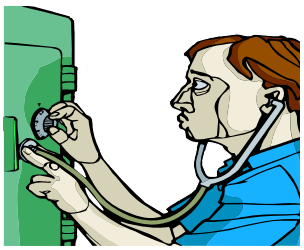
Security vs. efficiency

- Cryptographic commitments: several modular multi-exponentiations over large numbers
- OBU platform: NXP ARM7 microcontroller (32 bit) / SW
- Highest level of security cannot (yet) drive on German highway

OBU timings and speed tolerance for a 1-hour journey

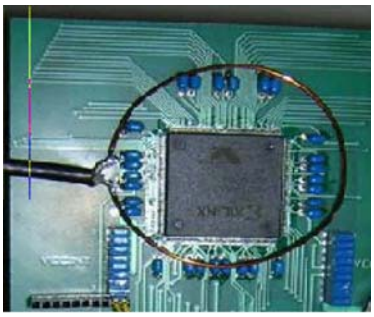
Security / Operation	Low (512 bit)	Normal (1024 bit)	High (2048 bit)
Map-Matching	**839.11 s**		
One segment	**1.80 s**	**7.88 s**	**47.79 s**
Max. Speed	**1530 km/h**	**350 km/h**	**57 km/h**

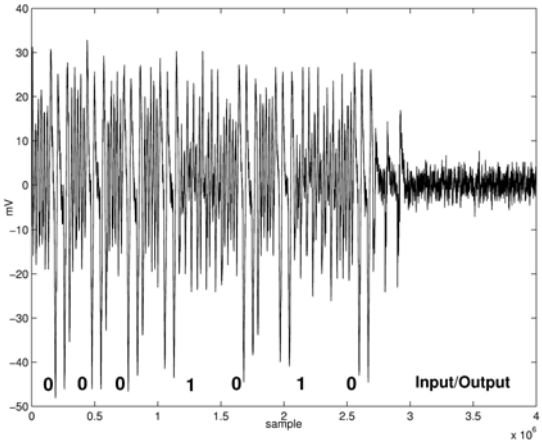
[slides courtesy: Josep Balasch]



2 Physical Security

Static CMOS tells everything it is doing!

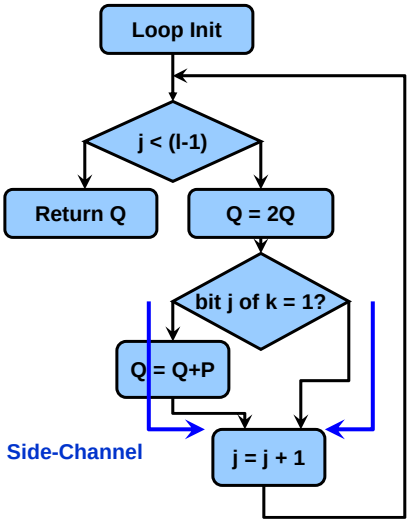




Insecure ECC implementation

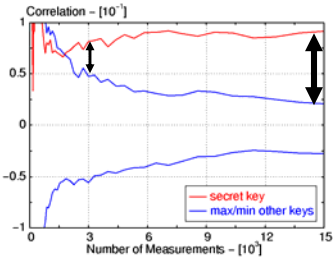
ECC point multiplication

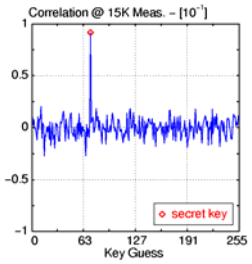
```
In: point P, key k (l bits)
Output: Q = k.P

for j = 0 to l – 1
   Q = 2.Q /* double */

   if (bit j of k) is 1
   then
      Q = Q + P /* add */
Return Q
```



Physical security

- *Physically Observable Cryptography*: standard “theoretical” basic assumptions do no longer hold
- But how do you measure the security of "Physically Observable Cryptography"? No real consensus yet ..
  - Information leakage
  - Measurements until disclosure





Solution approaches

- Example 1: “Provable physical security”= provably secure constructions under “physical assumptions”
  - e.g. “constrained side-channels attacks are possible”
  - e.g. “tamper resistant primitives exist”
- Example 2: Side-channel resistant circuit styles integrated in standard cell place & route
  - e.g. Wave dynamic differential logic (WDDL)

(EDA) design challenges

- Physical trust can be achieved with countermeasures, but most are ad hoc.
  - A countermeasure against one attack can open door to another attack (See HOST 2010 next door, Monday morning, 9am)
- Need a holistic design approach
- Start from trust anchors = roots of trust
- Build-up a security application

Conclusions

- Security challenges:
  - Many players in the field: government, business and customers
  - Different stakeholders have different interests; when these are conflicting or contradicting, security issues may arise
  - In-depth security analysis required
- Smart meter, smart grid can learn from other ICT security applications:
  - Privacy in social networks, in road-tolling and other ICT applications
  - Implementations will need Physical Security and Tamper resistance
  - Network issues

Reading

- J. Balasch, I. Verbauwhede, and B. Preneel, "An Embedded Platform for Privacy-Friendly Road Charging Applications," In Design, Automation and Test in Europe (DATE 2010), IEEE, pp. 867-872, 2010.
- J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," accepted for publication USENIX, August 2010.
- www.cosic.be publication list
- IBBT project, NextGenITS